Bulletin d'information 2ème semestre 2010 - N° 35

AMICALE MEMOIRE DU RESEAU GALLIA

RESEAUX : GALLIA – R.P.A. – DARIUS – DUPLEIX – REIMS – COTY MARGUERITE - CYPRIEN - CENTRES D'ANTENNE – LORRAIN

SIEGE : 4, Tournemotte 03000 NEUVY lès MOULINS C.C.P. : 532796 G PARIS

Tél. et FAX : 04 70 46 18 50 - reseaugallia.org - memoiregallia@wanadoo.fr

Le mot du Président

Assemblée générale 2010

Ce bulletin contient le compte rendu de notre Assemblée générale de 2010. Après l'approbation du rapport moral et du rapport financier, j'ai eu le plaisir de féliciter leurs auteurs en ces termes :

j'ai à adresser, de ma part et de la vôtre, des remerciements et des félicitations aux deux auteurs de ces rapports annuels, qui résument l'activité qu'ils ont déployée pour que notre Amicale continue à vivre et à bien vivre.

Le site GALLIA, que Jacques DIEU a mis en place et qu'il anime, est le support essentiel de cette vie.

Si l'on compare l'impact de ce site à celui de notre Journal, qui, depuis plus de 60 ans, a constitué un lien entre les « GALLIA », on perçoit une différence de nature et d'importance de la diffusion en faveur de ce support, grâce à son enrichissement continu et à son ouverture à tous les internautes sympathisants, en particulier à ceux qu'y mènent des rebondissements depuis d'autres sites touchant la Résistance.

Le nombre de visiteurs recensé en est la preuve magnifique.

Notre Secrétaire général a donc su utiliser les prodiges de l'informatique pour assurer cette démultiplication de la mémoire de GALLIA. Jusqu'à présent, c'est en fouillant dans les archives jaunissantes ou des anciens numéros de notre journal que nous tentions, souvent en vain, de répondre à des questions que posent des anciens, leurs descendants, ou des chercheurs. L'informatisation rend cette recherche plus facile et plus efficace, et permet de la coupler à d'autres travaux de mémoire.

Pour illustrer la révolution de nos comportements, même de notre façon de vivre, suscitée par notre intrusion dans un monde digital virtuel, imaginons ce qu'aurait été notre travail d'agent de renseignement s'il, avait pu être informatisé… : l'envoi par Internet au BCRA à Londres de la photographie d'une installation ennemie (prise grâce à un téléphone mobile et scannée) aurait été immédiat, alors que ce genre de document ne lui parvenait en 1943 ou 44 qu'après avoir rebondi d'une boîte aux lettres à une autre puis avoir attendu une lunaison favorable pour être embarqué à bord d'un petit Lysander ! Et puis, malgré leur complication et leur efficacité démontrée, les systèmes de codage dévoilés dans ce bulletin sont dépassés par les possibilités actuelles de l'informatique.

Abandonnons ce thème facile d'histoire-fiction anachronique et laissons Internet prolonger notre travail de mémoire, qui a pris grâce à Jacques DIEU un nouveau souffle.
Bon vent au site GALLIA !

Bernard LEVI

LA CRYPTOGRAPHIE *D'HIER...*

Le terme "cryptographie" provient du grec *Kruptos*, "caché", et de *graphein*, "écrire".

Cryptographie : ensemble des procédés permettant de transformer un message écrit, dit *clair*, en un autre message, dit *chiffré*, ou *crypté*. (Hachette Multimédia).

La cryptographie a une histoire :

Le premier "document" crypté connu remonte à l'antiquité. Il s'agit d'une tablette d'argile retrouvée en Irak, et datant du XVI ème siècle av. J.C.. Un potier y avait gravé sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots.

La technique assyrienne

Entre le XXème et le VIIème siècle av. J. C., on utilise un Scytale ou bâton de Plutarque pour encrypter les messages. Seul une personne, disposant d'un bâton de diamètre identique à celui ayant servi à écrire le message, peut le déchiffrer.
La principale faiblesse de ce système réside dans le fait qu'un bâton d'un diamètre approximativement égal suffit à déchiffrer le texte. La sécurité réside donc sur le secret autour du procédé d'encrytage.

Nabuchodonosor

Au alentours de 600 ans av. J.C., Nabuchodonosor, roi de Babylone, employait une méthode originale : il écrivait sur la crâne rasé de ses esclaves, attendait que leurs cheveux aient repoussé, et il les envoyait à ses généraux. Il suffisait ensuite de raser de nouveau le messager pour lire le texte.
On remarque dans ce procédé une certaine fiabilité : en effet, l'interception du message par un tiers est tout de suite remarqué.

Les premiers "vrai" systèmes de cryptographie

Il faut attendre 200 av. J.C. pour voir apparaître les premiers "vrai" systèmes de cryptographie. Ce sont essentiellement des chiffres par substitution.

Il en existe de 4 types :

- Substitution mono-alphabétique : remplace chaque lettre du message par une autre lettre de l'alphabet,

- Substitution homophonique : fait correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères,

- Substitution poly-alphabétique : utilise une suite de chiffres mono-alphabétique (la clé) réutilisée périodiquement,

- Substitution de polygrammes : substitue un groupe de caractères dans le message par un autre groupe de caractères.

Le code de César

Jules César (en latin Caius Julius Caesar) Homme d'Etat et général romain (Rome, vers 101 av. J.C. – 44 av. J.C.).
Le code de césar est la méthode cryptographique, mono-alphabétique, la plus ancienne communément admise par l'histoire. Son système est simple, il consiste à décaler les lettres de l'alphabet d'un nombre n. Par exemple, si on déplace A par D (n=3), on remplace B par E, C par F, etc... Pourtant sa simplicité conduisit les officiers sudistes à le réemployer durant la guerre de Sécession. L'armée Russe en fit de même en 1945.

Le carré de Polybe

Polybe, historien grec (env. 200 – 125 av. J.C.), est à l'origine du premier procédé de chiffrement par substitution homophonique.
C'est un système de transmission basé sur un carré de 25 cases (on peut agrandir ce carré à 36 cases, afin de pouvoir ajouter les chiffres ou pour chiffrer des alphabets comportant davantage de lettres, comme l'alphabet cyrillique).

LA CRYPTOGRAPHIE *D'HIER…*

E français, on supprime le "W", qui sera remplacé par "V". Il existe une variante ou ce sont "I" et "J" qui se partagent la même case. Chaque lettre peut être ainsi représentée par un groupe de deux chiffres : celui de sa ligne et celui de sa colonne. Ainsi "e" =(1;5), "u" =(5;1), "n" =(3;4), …

Polype proposait de transmettre ces nombres au moyen de torches. Une torche à droite et cinq torches à gauche pour transmettre le lettre "e" par exemple. Ce procédé permettait donc de transmettre des messages sur de longues distances.

Le chiffrage de Vigenère

Blaise de Vigenère (1523 – 1596) est l'auteur d'un des premiers systèmes "à mot de passe", c'est-à-dire un système de substitution poly-alphabétique. Cette méthode domina trois siècles durant.
Le texte chiffré s'obtient en prenant l'intersection de la ligne qui commence par la lettre à coder, avec la colonne qui commence par la première lettre du mot de passe, et ainsi de suite. Dès que l'on atteint la fin du mot de passe, on recommence à la première lettre. Pour décoder, il suffit de faire la même chose dans l'autre sens.
Cet algorithme de cryptographie comporte beaucoup de points forts. Il est très facile d'utilisation, et le décryptage est tout aussi facile si on connaît la clé. La grande caractéristique du chiffre de Vigenère est qu'il est impossible de retrouver où sont certaines lettres. Un autre avantage réside dans le fait que l'on peut produire une infinité de clés.

Le chiffre de Delastelle

L'inventeur de ce système est un français nommé Félix-Marie Delastelle (1840 – 1902).
Le chiffre de Delastelle diffère peu de celui de Polype La plupart de ces méthodes sont de simples adaptations de méthodes existantes.

La machine Enigma

L'histoire de la machine Enigma commence en 1919, quand un ingénieur hollandais, Hugo Alexander, dépose un brevet de machine à chiffrer électromécanique. Ses idées sont reprises par le Dr Arthur Scherbius, qui crée à Berlin une société destinée à fabriquer et à commercialiser une machine à crypter civile : l'Enigma. Cette société fait un fiasco, mais la machine Enigma a attiré l'attention des militaires allemands dès 1925. Les Allemands y croient dur comme fer. Ils vont construire 30 000 machines de ce type.
Le codage Enigma effectué par la machine Enigma est à la fois simple et astucieux. Chaque lettre est remplacée par une autre, l'astuce est que la substitution change d'une lettre à l'autre.

Pour l'essentiel de ses points forts, c'est le nombre de clés énorme, et la réversibilité : si, avec la même clé secrète initiale, on tape le message clair, on obtient le message codé, et avec le message codé, on obtient le message clair.
Cependant, elle a une faille dans la clé du codage, celle qui détermine la configuration initiale des brouilleurs. Jamais la lettre A ne sera codée par un A.
Une des autres faiblesses dépend plutôt du protocole utilisé par les Allemands : certains opérateurs (par exemple, ceux qui informaient la météo) prenaient peu de précautions et commençaient toujours leurs messages par les mêmes mots (typiquement "Mon général …"). Les Anglais connaissaient ainsi pour une partie du message à la fois le texte clair et le texte codé, ce qui aide à trouver la clé. Et comme c'est la même clé qui sert pour toutes les machine Enigma de l'armée allemande pour un jour donné, une erreur de protocole dans un message peut compromettre la sécurité de toutes les autres !

Remerciements pour la participation de Messieurs GUITTENY Julien – LEDANOIS Mathias– LORET Guillaume - TA David du site cryptotpe

LA MACHINE A CHIFFRER *ENIGMA*

"Les soldats se battaient sur les champs de bataille partout dans le monde, sous les bombes et les balles. Mais les services de renseignements de chaque pays se livraient à une autre guerre intellectuelle cachée aux yeux du monde.

Dans les années 1940, la cryptographie atteint de nouveaux sommets, inimaginables seulement quelques années avant. Avec l'invention de nouvelles machines d'encodage, une nouvelle génération d'encodeur vit le jour.

La Pologne surveille son voisin

Les principales découvertes en matière de décodage et d'encodage eurent lieu avant même l'ascension d'Hitler au pouvoir. Dans les années 1920, la Pologne commença à intercepter des transmissions codées allemandes, elle rassembla une équipe de mathématiciens pour les déchiffrer. A ce moment là, les Allemands encodaient leurs messages avec une machine très sophistiquée nommée Enigma. Elle fut développée par Arthur Sberbius en 1918. Cette machine utilisait le principe suivant : trois roulettes rotatives qui permutaient les lettres plusieurs fois. Même si une puissante ennemie parvenait à voler une machine Enigma et à comprendre son fonctionnement, ils ne pourraient déchiffrer les messages sans savoir la séquence d'encodage choisie par l'opérateur de la machine. Grâce à ce système, il y avait environs 15 milliards de séquences d'encryptage possibles, le code émis par Enigma était donc incassable. Du moins, c'est ce que croyaient les Allemands.

Ils ont cependant commis une erreur cruciale dans la politique opérationnelle d'Enigma. Pour éviter des erreurs dues aux mauvais signaux radio ou aux interférences, les opérateurs allemands devaient transmettre la séquence d'encodage deux fois. C'est ce qui manquait aux mathématiciens polonais pour déchiffrer le code. Les mathématiciens Marian Rajewski, Henryk et Jerzy Roycki étaient les principaux chercheurs au Bureau Polonais du Chiffrage. Ils permirent à la Pologne de clairement lire les messages allemands dès 1933. Rajewski accumula tellement de connaissances sur la machine qu'il put en construire une lui-même, mais la Pologne garda ses renseignements top-secret, sachant que si les Allemands avaient des doutes sur la sécurité de leur système, ils en développeraient un nouveau, ce qui obligerait les spécialistes à tout recommencer de zéro.

Le secret est divulgué

Lorsque Hitler annula son traité de non-agression avec la Pologne en 1939, les Polonais surent qu'ils devaient partager leur secret. Ils entrèrent en contact avec les services de renseignements britannique et français, ils leur apprirent qu'ils possédaient une machine à chiffrer allemande et qu'ils savaient comment déchiffrer les messages allemands. Ils fabriquèrent donc des répliques d'Enigma pour les Britanniques et pour les Français. Lorsque les troupes allemandes envahirent la Pologne cette année là, le centre de décryptage fut déménagé en France et à Bletchley Park, en Angleterre.

Lorsque les Allemands rajoutèrent deux robots à la machine, le décryptage des messages devint beaucoup plus ardu. Au début de la guerre, 120 personnes travaillaient à Bletchley Park, plusieurs milliers y travaillaient en 1944. En Grande-Bretagne, le programme Enigma fut baptisé "Alan Turing Spearhead Ultra" (fer de lance Alan Turing). En 1940, les Britanniques pouvaient décoder les messages de la Luftwaffe, ceux de la marine furent brisés dès 1941.

La prise de l'U-33

La récupération de trois rotors Enigma sur l'U-Boat U-33 le 12 février 1940, en mer d'Irlande, aida grandement la recherche alliée. Le navire britannique H.M.S. Gleaner intercepta l'U-33 alors qu'il allait poser des mines dans un chantier portuaire britannique. Le Gleaner largua des mines sous-marines sur le sous-marin allemand, ce qui le força à faire surface. Le Glearner percuta l'U-33 ce qui força le capitaine du sous-marin à ordonner le sabordage du navire. L'un des hommes de l'U-33 ne pu suivre l'ordre de jeter les rotors à l'eau, les Britanniques purent donc mettre la main sur ces pièces précieuses. Peu après, les chercheurs de Bletchley Park cassèrent les codes d'Enigma, les Britanniques partagèrent leurs connaissances avec les alliés américains (en retour, les Alliés partagèrent leurs connaissances sur le cryptage japonais). En 1943, les Alliés pouvaient suivre de près les mouvements allemands sur terre, sur mer et dans les airs. Les Alliés purent garder ça secret, les Allemands continuèrent donc à croire que le code Enigma était toujours incassable.

La fin de l'histoire

Ce succès en matière de renseignements militaires influencera énormément le cour de la Seconde Guerre mondiale. La capacité des Alliés à déchiffrer les transmissions de la marine italienne, effectuées avec Enigma, leur donna l'avantage lors de la bataille de Matapan (au large de la Crête), cette victoire clef écartera la menace italienne de la Méditerranée. Les informations décodées permirent également de connaître à l'avance les mouvements des troupes de Rommel en Afrique du Nord. Le décryptage permit aux Alliés d'apprendre que les fusées V1 étaient fabriquées à Peenemüde en Allemagne, ce qui donna lieu à un raid sur ces usines. Cela permit de libérer la voix pour l'Opération Overlord (la bataille de Normandie) et pour l'Opération Anvil Dragoon (la bataille de Provence) pour l'invasion de la France en juin et août 1944."

La cryptographie a toujours été utilisée par les gouvernements, l'armée et les services de renseignement. Pourtant, la première utilisation démilitarisée remonte à 1976 avec le DES (Data Encryption Standard : créé par IBM et le NSA - il est l'algorithme de chiffrement le plus utilisé au monde durant le dernier quart du XX^{e} siècle).

1976, cette année est considérée comme l'année de commencement de la cryptologie moderne. Elle marque en effet le début de la cryptographie sûr, et destinée à tous.

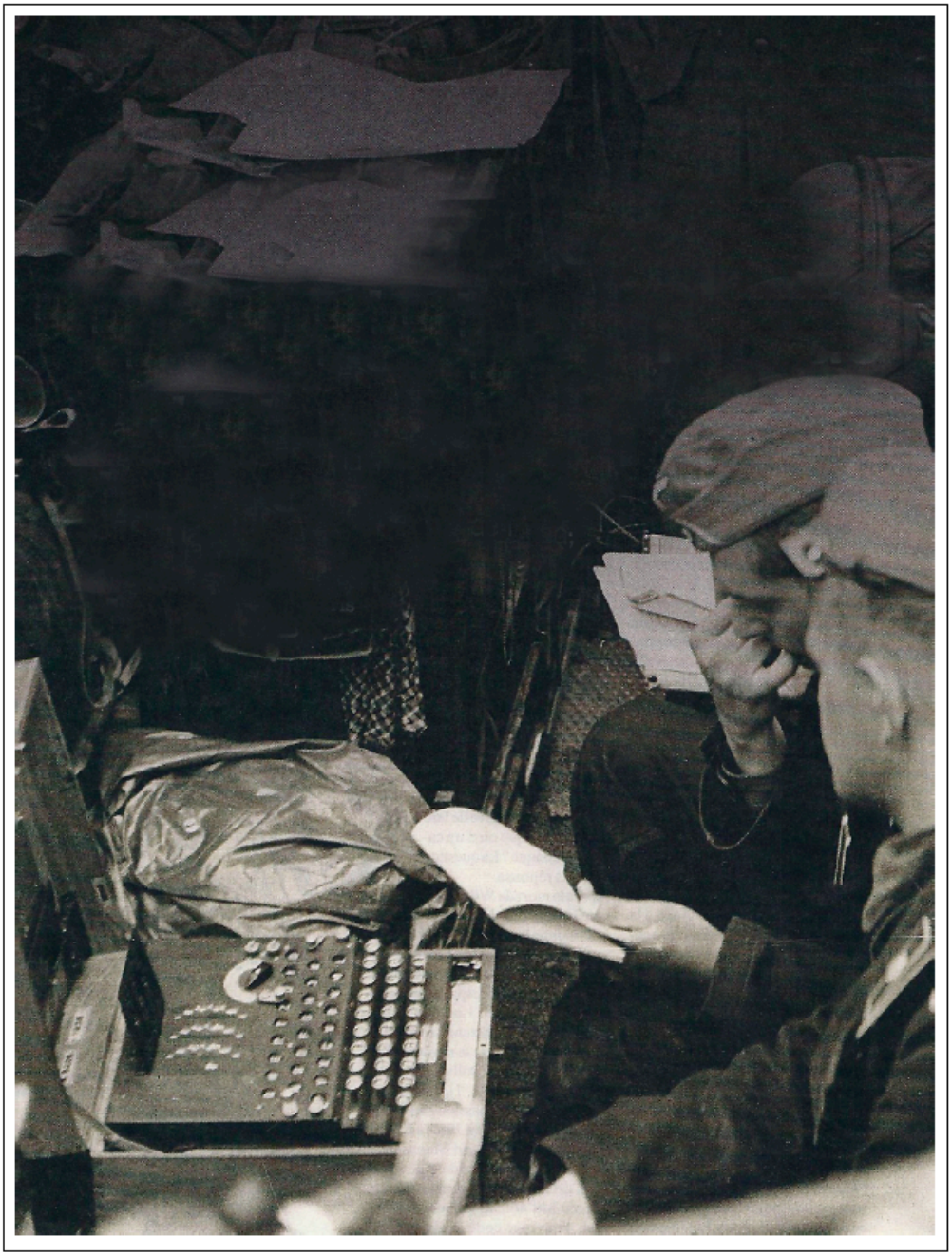
Mais la cryptographie répond aussi à un besoin de confidentialité croissant depuis Internet. Avec le flux d'informations permanent, la sécurisation des échanges est devenue un enjeu majeur dans notre société, que ce soit pour la télévision (Canal+, TPS, ...), les cartes bancaires, les moyens de communications (réseaux pour GSM, Internet, ...), etc. Les Etats, les entreprises, et certains particuliers utilisent déjà le cryptage pour sécuriser leurs échanges. En effet, le cryptage est devenu un simple outil que tout le monde utilise et beaucoup sans le savoir.

La Cryptographie est donc un moyen efficace de protéger les échanges simplement.

Des recherches sur de nouveaux procédés de cryptage ont lieu, notamment sur la cryptographie quantique (les atomes). La cryptographie quantique rendra inviolable les messages cryptés.

Sources : nos remerciements aux chercheurs : Julien GUITTENY, Mathias LEDANOIS, Guillaume LORET, David TA : cryptotpe.free.fr -

A consulter : Historia, *La clé des codes secrets*, n°714 juin 2006 - *Secret Défense, Histoire du Renseignement Militaire Français*, Parvulesco Constantin, Ed. Etai, (2007) - wikipédia.org/*Histoire de la cryptologie* - *Les Réseaux de renseignement franco-polonais*, Jean Medrala, L'Harmanttan - *secondeguerre.net* -



Soldats allemands envoyant à leur état-major des messages codés sur la machine *Enigma*

© Amicale mémoire du réseau GALLIA

RESEAU GALLIA-REIMS

RAPPORT SPECIAL DU 5 NOVEMBRE 1943

« SR

"Veuillez bien trouver ci dessous une étude de 4444 (*immatriculation de l'agent du réseau REIMS*) sur deux codes secrets allemands dont je vous donne la clé.

Les éléments de ces codes m'ont été donnés par 4614, sous les ordres du chef régional de Toulouse, 4611 (*Poncelet Guy, ancien sous-préfet.*

Ils émanent de deux agents français du SR allemand, actuellement en fuite et que le service Reims a fait passer en Espagne où je vous serais gré de vouloir bien vous intéresser à leur sort pour autant que la chose soit possible.

Le principal de ces agents m'a remis le rapport suivant :

Le 26 octobre 1943

Le soussigné Bardelou Guy, Officier de Marine, ayant travaillé à Marseille comme collaborateur direct de l'ingénieur en chef Hinze Hartwig, certifie pouvoir fournir tous les détails sur les chantiers en cours dans la région marseillaise, entre autres les chantiers de Rove (base sous marine souterraine) et de la Redonne (observation et batteries lourdes en projet) et de multiples détails sur les divers chantiers en cours dans la région, les fortifications et les défenses anti chars de la ville.

J'étais avant l'occupation de la zone sud, en relation avec Talon Gaston, ancien adjudant de cavalerie, ancien écuyer à Saumur, agent double qui était en rapport avec le capitaine Legendre du SR de Toulouse. Par son intermédiaire, j'ai réussi à m'infiltrer dans le SR allemand. J'ai été sous les ordres de Max Stoeklyn, suivre un cours à Paris. Ce service était dissimulé dans les bureau d'une agence soi-disant commerciale à l'en tête de B.E.M.I.C., 1 rue Lord Byron, tél. Balzac 3341. Après mon instruction, je devais être envoyé en Afrique du Nord avec un poste de radio.

J'ai donc été initié au chiffre. J'en connais deux, dont l'un est immuable et concerne les agents travaillant dans les colonies lointaines tandis que l'autre est encore en cours jusque fin décembre. Je n'ai pu, et pour cause, aller en Algérie car j'ai toujours tergiversé en ne voulant pas quitter la France car mon utilité eut été nulle. En désespoir de cause, j'ai été envoyé à Marseille où, comme couverture, on m'a fait entrer comme ingénieur à l'organisation Todt. Mes relations avec Talon Gaston ont brusquement cessé. J'en ignore la cause. Je me suis mis en rapport avec un groupe de patriotes à qui je faisais part de mes observations qui, selon eux, étaient transmises. Malheureusement, l'un d'eux nommé Adrien Lamy, s'étant fait arrêté, j'ai dû quitter précipitamment Marseille, car j'y étais recherché par la Gestapo. J'étais en rapport à Marseille avec un officier du nom de Reuter, qui se faisant appeler Vernon et qui habite actuellement Hôtel de la Méditerranée, chambre numéro 10.

Bardalou – 40 173 Marseille.»

Précisions du Bureau Central de Renseignement et d'Action – Londres :
Bardalou Guy Emilien, né à Constantine (Algérie) le 30 octobre 1912. Officier de marine marchande – Enseigne de vaisseau de réserve – mobilisé le 25 août sur le P 6 "Caraïbe" – démobilisé le 27 décembre 1940 à Diego Suarez (Madagascar) – Croix de guerre 39-40 – immatriculé 40 173 secteur de Marseille.

ETUDES DE L'AGENT DE RENSEIGNEMENT *4444*

« CODE N° I.

Durée de validité : serait immuable.

Usagers : agents français du SR allemand travaillant sur les colonies françaises.

Clé : simple transposition de lettres.

Si les renseignements que je possède sont complets et exacts, ce code n'a qu'une valeur bien faible. Aucun officier de chiffrement n'éprouvera la moindre peine à décrypter. Les lettres à utiliser pour la transposition sont tirées du texte des premiers essais de philosophie de Victor Cousin, édition de 1873. Je joins cet ouvrage en annexe en attirant votre attention sur le fait qu'il n'a pas été soustrait aux services allemands, mais acheté dans le commerce non sans grandes difficultés, cela va de soi.

Au premier juillet 1943, le texte utilisé pour la transposition était la première page de l'ouvrage, étant entendu que la préface, l'avertissement, les titres et sous-titres des chapitres ne rentrent pas en ligne de compte.

La première page, utilisée le 1er juillet est donc le début du discours du 7 décembre 1815. Par la suite, avancez d'une page chaque jour.
Exemple : la page utilisée le 8 août est la page 59 de l'ouvrage.
Supposons que nous soyons au 1er juillet. On écrit à la suite l'une de l'autre 26 lettre tirées du texte en commençant bien entendu par le début de celui ci, en haut de la page, mais en ayant soin de laisser tomber chaque fois une lettre qui aurait déjà été utilisée.

Donc, au 1er juillet, pour le texte :
"Lorsque appelé à faire paraître dans ses fonctions plus élevées la mâle éloquence et cette vigueur de sens et de dialistique qui marquaient son enseignement, l'homme illustre que vous avez tant de fois applaudi dans cette enceinte, etc ...
On soutient l'alphabet fantaisiste suivant :
LORSQUEAPFITDNCVMG... etc... et, par exemple, le 21 septembre (page 80 de l'ouvrage), pour le texte :
"scepticisme de Berkeley et de Hume, etc..., nous avons par la transposition :
SCEPTIMDRKLYHUNAFQVJOGXZW. Chacune de ces 26 lettres, prises dans leur ordre vaut, tout simplement, pour la transposition, la lettre correspondante à l'alphabet régulier, soit :
SCEPTIMDBRKLYHUNAFQVJOGXZW
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Soit le 21 septembre à coder la phrase :
Faite parvenir au plus vite détails sur ...etc. On aura :
ISBV TQNS FOTH BF SJ, etc... ce qui me paraît beaucoup plus simple.
Le télégramme est expédié par groupes de quatre lettres. Pour les chiffres, on les remplacent par les lettres initiales de chaque ligne du texte, toujours en sautant les lettres déjà employées et en recherchant trois lettres différentes pour le O. Soit, toujours au 21 septembre (page 103 de l'ouvrage) : septicisme de... que sauver... pour pouvoir... théorie des... etc. ce qui donne :
SQPTDSMRCLVA
123456789000
Le radio émetteur appelle l'indicatif du récepteur, par exemple DPBC. Dès que le DPBC est en contact, il répond par l'indicatif de la journée réservé au récepteur. Cet indicatif est de trois lettres : ce sont les trois lettres initiales des dernières, avant-dernières et antépenultiennes lignes du texte "du jour", soit, toujours le 21 septembre.
science ou à une autre...
Va se convertir... de se convertir...
soit l'indicatif DVS, toujours avec cette restriction que l'on saute une lettre déjà employée. »

Le poste émetteur répond alors par l'indicatif de la journée réservé à l'émetteur. Cet indicatif est tiré des mêmes lignes de texte mais il est constitué par les lettres terminales de ces lignes, soit le 21/9 : incertitude de Reid
...entre les mains de ses successeurs
il y a ici une lettre dédoublée, s, il faut donc remonter une ligne plus haut où l'on trouve la lettre n, soit l'indicatif SDN. Les radios sont ainsi d'accord sur le texte qui a été employé et la transmission du télégramme peut se faire.
Les trois premiers groupes de ce télégramme sont réservés :
Le premier à l'heure d'émission, par exemple 0904 signifie le 4 septembre.
Le troisième à la numérotation du télégramme : 3 chiffres et une lettre, soit par exemple 485U.

CODE N° 2

Durée de validité : jusqu'au 31 décembre 1943.
Usagers : agents français du SR travaillant en France
Clé : double transposition de lettres basée (ce sur la date et sur le communiqué allemand du jour en sa traduction française intégrale et officielle.
Au contraire de l'autre, ce code donne une transposition qui rend les messages indécryptables si l'on n'en possède pas la clé.
Je joins pour la facilité des opérations l'échelle alphabétique fixe et l'échelle alphabétique mobile qui peuvent ici tenir lieu de grilles.
Soit à coder, le 29 octobre, la phrase : viendrai demain huit heures.
La 29ème lettre de l'alphabet est la lettre C (26+3) et ce jour là, le communiqué commence traditionnellement par les mots : le haut commandement des forces armées allemandes communique... (négliger la date et la mention du quartier général du F.). Placer la lettre clé C de l'échelle mobile en face de la première lettre à coder sur l'échelle fixe, soit, dans l'exemple cité le C de l'échelle mobile en face du V de l'échelle fixe, on obtient :
ECHELLE FIXE :
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ

ECHELLE MOBILE : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Chercher ensuite sur l'échelle mobile la première lettre du communiqué allemand : la lettre L : elle se trouve en face de la lettre E de l'échelle fixe : La lettre E remplacera donc dans le texte la lettre V. Placer ensuite la lettre clé C en face du second signe à coder, soit la lettre I.
On a :
ECHELLE FIXE :
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOP QRSTUVWXYZ
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Chercher sur l'échelle mobile la deuxième lettre du communiqué allemand du jour, la lettre E : elle est en face de la lettre K de l'échelle mobile :
K, en code remplace donc I et ainsi de suite.
La transposition étant double, il est impossible de décrypter en se basant sur la fréquence des signes. On comprendra en effet que la lettre E pourra dans le texte codé être remplacée tantôt par un K, tantôt par un V, tantôt par n'importe quelle lettre de l'alphabet suivant ce que sera la lettre correspondante du communiqué allemand :

Les chiffres sont représentés immuablement par les lettres suivantes :
1 1 2 2 3 4 5 6 7 8 9 0 0 0
L E G I O N F R A C S D M B
Tirées de la sentence :
"Légion française des combattants", les lettres déjà employées étant sautées.
Les cinq premiers groupes du télégramme (décomposé en groupe de 4 lettres) sont réservés :
Le premier à la date, comme pour le code 1
Le second pour l'heure, comme pour le code 1
Le troisième au nombre de lettres du télégramme, par exemple 0954
Le quatrième au numéro en quatre chiffre, par exemple 1143
Le cinquième à un groupe spécial de contrôle.
REIMS.»

(A ce rapport, était ajouté un paragraphe concernant la situation du réseau en octobre 1943.)

« ADMISTRATION.

GALLIA et II FC connaissent par 4445, les détails de l'accident survenu le 18 octobre au secrétariat central du réseau Reims. Etant à cette époque sur le terrain d'opération, je ne pourrai vous fournir aucun détail sur cette affaire qui ne soit mieux connu de 4445, que moi-même.
Mais, je tiens avant tout à faire remarquer que personne n'étant arrêté et les archives du service ayant été sauvées grâce au sang froid et au dévouement de 4459, la dernière action de la Gestapo n'a rien amené d'irrémédiable. Les différents SR Reims fonctionnent très normalement et transmettent régulièrement les rapports hebdomadaires.
Une première série de ces rapports hebdomadaires a déjà fait l'objet d'une synthèse et je prie 4447 de la transmettre dès qu'en possession des archives, il pourra y amener les croquis et divers documents annexes.
Deux autres séries sont au secrétariat du PC et demandent à être dactylographiées en un rapport unique de synthèse.

Malheureusement, le matériel et le personnel nous font actuellement complètement défaut. J'espère dans un délai relativement court, par 4447, couper court, à cette situation mais en attendant, je ne puis que demander de l'indulgence à l'égard des retards accusés par le réseau dans la transmission du courrier.

4445 - 4446 et 4459 font l'objet d'une mesure d'évacuation par le Sud. Pour liquidation de leurs dossiers, je vous transmets en annexe leurs fiches biologiques.

Je demande à II FC de vouloir bien rappeler à l'Administration de la Sûreté Belge que 4445 et 4459 sont militaires de carrière et qu'entrés au service le 1er décembre 1942, ils ont, si je m'en rapporte aux promesses de Pierre Muret, droit à la consignation de leur traitement en banque de Londres, depuis la date de leur engagement.»

COURS DE L'HISTOIRE

DE LA

PHILOSOPHIE

MODERNE

PAR

M. VICTOR COUSIN

Nouvelle édition, revue et augmentée

PREMIÈRE SÉRIE

TOME I

Histoire des principaux systèmes de la philosophie moderne sur la question de l'existence personnelle.

Histoire des principaux systèmes de la philosophie moderne et particulièrement du système de Kant sur la nature, l'origine et la légitimité de nos connaissances dans l'ordre intellectuel et dans l'ordre moral.

Fragments divers relatifs aux leçons précédentes.

BODLEIANA BIBLIOTHECA

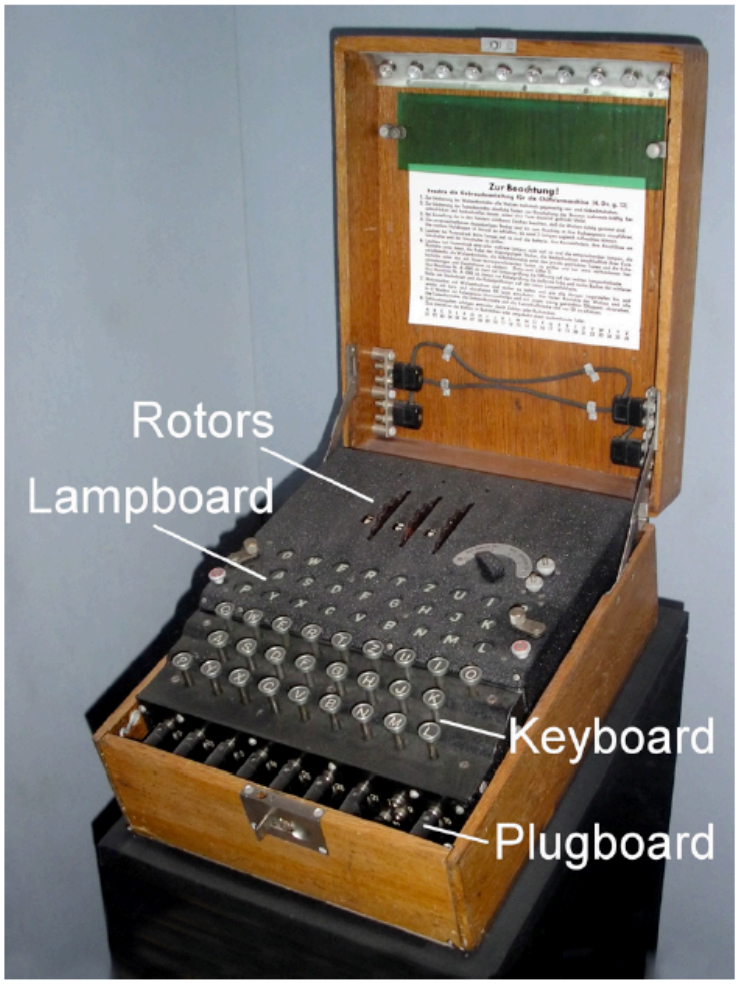
PARIS

LADRANGE, ÉDITEUR, 19, QUAI DES AUGUSTINS. — LIBRAIRIE DE DIDIER, 35, QUAI DES AUGUSTINS.

265 f. 21

Victor Cousin est un philosophe et homme politique français, né à Paris le 28 novembre 1792 et mort à Cannes (Alpes-Maritimes), le 14 janvier 1867.
Philosophe spiritualiste, chef de l'école éclectique, il édita les œuvres de Descartes, traduisit Platon et Proclos, écrivit une *Histoire de la philosophie au XVII^e siècle* (1829), *Du Vrai, du Beau et du Bien* (1853), et plusieurs monographies sur les femmes célèbres du XVII^e siècle.

LA MACHINE ENIGMA



Musée Impérial de Londres

Pour percer ce procédé de cryptage, le service de renseignement français, recrute une "taupe" au sein du service allemand du chiffre : Hans Thilo Schmidt, sous le pseudonyme de "HE". Il livra, moyennant finances, les clés mensuelles d'Enigma, aussitôt transmises aux Polonais.

Président : M. LÉVI Bernard – Secrétaire général et rédacteur du bulletin et du site : M. DIEU Jacques - Trésorier : M. SCHMIERER Yves
Conseil d'administration : M. ARNOULT Henri - M. CARON Michel - M. CARRIÈRE Louis – M. COUTHERUT Michel - M. GENTIL Pierre - Mme FAURIAT Colette –
Achevé d'imprimer sur les presses de l'Imprimerie Alpha Numérig' rue Bad Vilbel, Moulins sur Allier 04 70 20 09 92

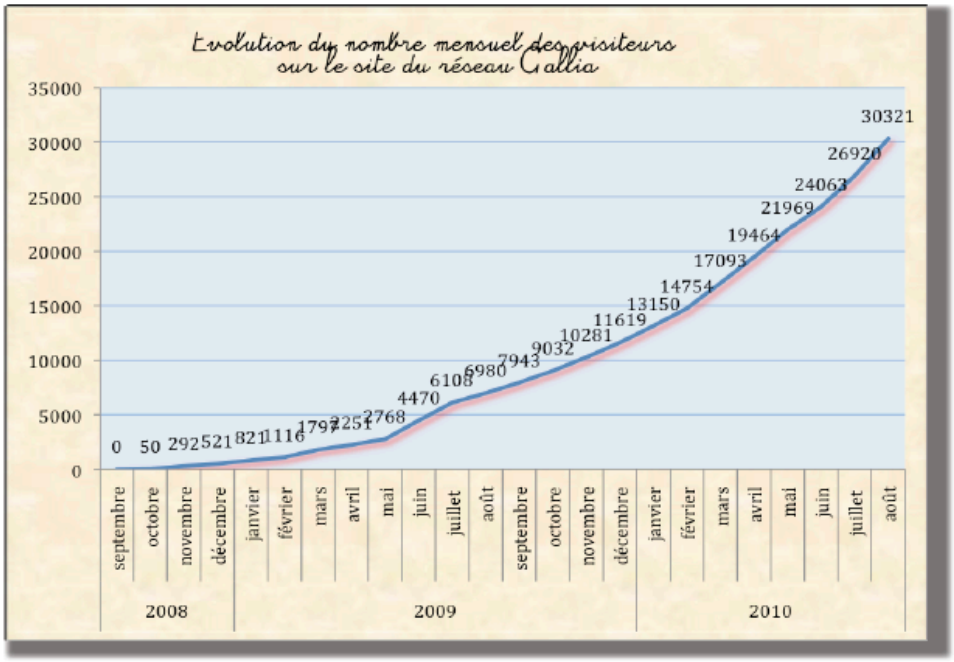
© Amicale Mémoire du Réseau GALLIA

Bulletin d'information -supplément

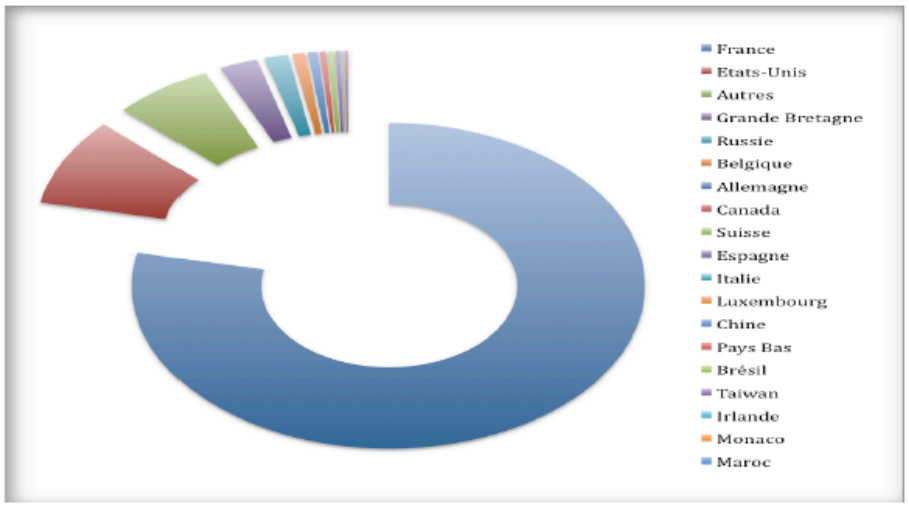
2ème semestre 2010 - N° 35

AMICALE MEMOIREDU RESEAU GALLIA

Aperçu statistique du site reseaugallia.org



Pays des visiteurs



ASSEMBLEE GENERALE
DE L'AMICALE MEMOIRE DU RESEAU GALLIA
Samedi 19 juin 2010
Au Club de la Fondation de la France Libre
59, rue Vergniaud 75013 Paris

Sont présents à onze heures :
le Président Monsieur LEVI Bernard
le Secrétaire général Monsieur DIEU Jacques
le Trésorier Monsieur SCHMIERER Yves
Madame DIEUDONNE Marie
Madame FAURIAT Colette
Colonel CARRIERE Louis
Monsieur CARON Michel
Monsieur GENTIL Pierre
Ils sont rejoints à treize heures par :
Madame CARRERE Josiane, puis
Monsieur ARNOULD Henri

Avant de passer à l'ordre du jour, Monsieur le Président propose de réexaminer la composition du Conseil d'Administration dont certains membres rencontrent des difficultés de déplacement et de créer le titre de « membre d'honneur ». A l'approbation de tous les présents sont nommés « membres d'honneur » : Monsieur LARRRERE Gérard - Monsieur MAIRE Auguste.

Acceptent d'entrer au Conseild'Administration :
Monsieur GENTIL Pierre
Madame FLAURIAT Colette.

1. Rapport moral

Monsieur le Secrétaire National rend compte de ses deux principales activités : le bulletin envoyé aux adhérents et le site Internet créé à l'issue de l'Assemblée Générale 2008.

1.1 Le Bulletin

En 2009 sont parus quatre numéros : le 30 consacré à un chef de secteur, Jean SCHLOCHOW, le 31 au Colonel GORCE-FRANKLIN et aux Q.G. de la Résistance Française à Londres, le 32 à un agent de renseignements à Berlin et le 33 aux opérations aériennes du B.C.R.A..
En 2010, le bulletin est devenu semestriel. Le numéro 34, traitant de l'organisation d'un réseau a été fait et envoyé, le numéro 35 s'attachera à l'utilisation du codage des messages utilisé par l'Etat-Major allemand.
Monsieur le Secrétaire national souligne les difficultés rencontrées, pour avoir accès aux archives, déposées, soit au château de Vincennes dépendant de l'Armée Française, soit aux Archives Nationales de France, il est précisé que nous avons les moyens financiers pour le coût des photocopies.

1.2. Le site Internet

Le site reseaugallia.org est de plus en plus fréquenté : 4.000 visites en 2009, 22.600 jusqu'à juin 2010, un réel succès. 500 personnes, qui se sont connectés, ont demandé des renseignements sur le site. Monsieur le Secrétaire répond au public du site, mais il est évident qu'une seule personne ne peut tout faire.

D'autre part, certains renseignements sont difficiles à manier, car ils relèvent du secret militaire. L'envoi du site à l'Elysée et au Ministère aux Armées a été fait.

Monsieur SCHMIERER se préoccupe de la responsabilité pénale, les droits d'auteur sur Internet n'étant pas régularisés. Monsieur le Président estime que l'assurance, d'un coût de 100 euros, ne doit pas, par précaution, être supprimée.

2. Rapport financier

Monsieur le Trésorier distribue le bilan financier de l'exercice 2009, dont le projet était joint au numéro 34 du bulletin, et le commente.

En 2008-2009, l'Amicale a reçu des dons généreux pour la création du site Internet, si bien que le solde positif était relativement important lors de la précédente Assemblée Générale. Il le reste à ce jour, de l'ordre de mille euros, mais avec une diminution de trois cent soixante-trois euros.par rapport à 2008

Il attire l'attention que pour l'exercice 2009 , seul trois bulletins ont été payés.

La facture du quatrième bulletin étant parvenue courant janvier 2010,son cout 169€ apparaitra dans le bilan 2010

Monsieur le trésorier rappelle que l'envoi régulier des cotisations, maintenues à quinze euros, reste l'essentiel pour le bon fonctionnement de l'Amicale.

Il souhaite que lui, soient envoyées en début d'année les cotisations 2011 et demande à ceux qui ne l'ont pas encore fait de s'acquitter de leurs cotisations 2010.

Il adresse aux donateurs le reçu réglementaire leur permettant de bénéficier d'une réduction d'impôt sur le revenu pour toute somme supérieure à 21€.

Il soumet à l'Assemblée le cas d'un Monsieur LANGUEPAIN, qui lui a fait parvenir un chèque de vingt euros, et souhaite adhérer à l'Amicale, car son père, médaillé de la Résistance, nommé préfet d'Alger à la Libération, travaillait pour le réseau GALLIA comme l'atteste la lettre d'un ancien membre du Réseau. Monsieur le Président estime que le test de la cotisation est un élément important et l'Assemblée Générale se prononce pour l'adhésion sous réserve de vérification des statuts.

L'Assemblée Générale approuve à l'unanimité le rapport moral et le rapport financier et donne quitus au bureau.

Monsieur le Président lit son mot à paraître dans le prochain bulletin et Monsieur le Secrétaire National offre aux participants la brochure qu'il a rédigée et éditée, avec l'aide du Ministère de la Défense par l'intermédiaire de l'Office National des Anciens Combattants et de la Fondation de la France Libre, « Autour du 18 juin 1940, à Moulins sur Allier … », à l'occasion du 70 ème anniversaire de l'Appel du Général de Gaulle.

Monsieur le Président remercie le Secrétaire et le Trésorier pour l'immense travail fourni afin que l'Amicale perdure et se fasse mieux connaître. Il lève la séance en invitant les participants à se retrouver autour d'un sympathique déjeuner.

La Secrétaire de séance Colette FAURIAT